Proceedings of the

International Safeguards Workshop: Design and Testing for High Reliability

15-17 October 2001

Brookhaven National Laboratory
Upton, NY, USA

EXECUTIVE SUMMARY

Prepared by
J. Lemley, A. Woodhead and M. Farnitano

The welcoming remarks by Brookhaven's Associate Director Ralph James highlighted the meeting's potential benefits. Participants would learn about the IAEA's difficulties in ensuring the reliability of remote-monitoring systems; the Agency would profit from the collective expertise of developers, users, and suppliers in evolving new solutions for reliability of instrumentation. The Workshop's objectives were successfully met; the outcome was most satisfactory due to the forthrightness of the IAEA's staff and the attendees' enthusiasm.

Nikolai Khlebnikov outlined the IAEA's expectations, and the importance of reliable integrated remote-monitoring systems in reducing the frequency of inspection visits to nuclear facilities under IAEA safeguards. IAEA equipment is reliable, often for up to 50 months in the field, though one or two systems fail yearly. The IAEA wanted practical, economic suggestions for designing, procuring, and life-long testing of systems, and for measuring properties of facility environments that might affect the performance of IAEA instrumentation. Max Aparo and Julian Whichello described the formal approach to categorizing, developing, documenting, and monitoring developmental projects including laboratory and field tests, vulnerability assessments, and measures taken to ensure that systems approach a seven-year service life. They outlined the problems that result from the IAEA’s being a small-scale buyer of both specialized and off-the-shelf components, while the large manufacturers lack interest in servicing the unique needs of such a small-volume customer. The foibles of vendors are troublesome, in failing to alert the IAEA to design changes, the rising costs of maintenance, lack of long-term guarantees, and dearth of spare parts, particularly for mission-critical equipment. They questioned whether the IAEA should require enhanced-reliability components and technology, and whether they could afford this approach to reliability. They sought opinions on fundamental issues, including using commercial products and Windows-based operating software, and the parameter ranges over which their environmental testing should be carried out. They deem it essential to measure environmental parameters during plant operation, and need advice on making measurements, and choosing equipment to simulate real operating environments. They briefly summarized their problems with single-event upsets (SEU), and their yearlong efforts that resolved many SEU problems.

Aparo described the work of his section in selecting, developing, installing, and repairing the IAEA's 25 different types of surveillance systems, six review systems, and associated software; there are too many systems, too thinly spread; many are obsolete; and components are mutually incompatible. There is a real challenge in deciding whether to select new, sophisticated, costlier equipment requiring specialized technical maintenance staff, or to opt for simple, less expensive, off-the-shelf products that can be maintained by generally trained technicians, and whether to acquire large inventories of spare parts. The Agency adopted a new cradle-to-grave approach for unattended monitoring systems that includes predictive rather than preventive maintenance, monitoring performance, and minimizing differing types of hardware and software. They plan to set up a database of environmental conditions found at specific facilities and various facility types, secure the long-term support of vendors, and establish state-of-health remote monitoring for instrumentation at remote sites.

Henry Tang spoke on the fundamental physics underlying radiation damage to instruments, the major sources of SEUs, key experiments, and predictive modeling. He described the genesis of an SEU from an alpha particle, cosmic-ray source, or thermal neutron, detailing how it temporarily perturbs the field gradients in an electronic device, creating a soft error undetectable by standard diagnostic tools that measure radiation damage. He offered calculations for determining the probability of an instrument's failure, and stressed the importance of developing cross-section-like data to understand neutron-induced SEU effects. Heather Dussault described her modeling of SEU effects in computer systems, explaining the inherent difficulties in such assessments. Thus, small changes in one part of a complex digital system might compromise other parts, affecting computations, execution sequences, synchronization of memory, and allowing uncommanded entrance into reserved modes. She used examples to suggest that the IAEA should closely examine the architecture of their systems and computers, and gave a thorough analysis of SEU effects on application programs, operating systems, compilers, and interpreters. Tang described his formulation for establishing failure rates in electronic instruments, which is less costly than lengthy Monte Carlo calculations.

Les Braby then discussed his approaches to radiation dosimetry, and SEU risk. He clarified the drawbacks of using neutron transport calculations to evaluate SEU rates and noted that many types of instruments are needed to measure the neutron spectrum inside and outside a reactor over the entire energy range that is relevant to SEU phenomena. He presented equations that showed how a large volume of low-density material (gas) could be used to simulate radiation effects in materials like silicon at densities typical of electronic circuits. His experimental method used a proportional counter filled with a low-density gas and having chamber walls containing silicon and other materials found in electronic circuits. Under the assumptions that response within an electronic device is independent of the spatial distribution of the ionization and that there is a threshold for the number of ion pairs required to create a SEU, this instrument can be used to measure the frequency of events above a defined threshold and predict the frequency of SEUs.

The focus moved to designing reliable instruments and testing them. Guenter Neumann described the Agency's problems with analog surveillance systems in the early 1990s, and their replacement with the digital systems utilizing the DCM 14 module. It underwent extensive environmental testing before it was authorized for field use; however *in situ* it showed poor reliability. Neutron-irradiation experiments uncovered the problems caused by SEUs from thermal neutrons. He considered ways to incorporate design features to mitigate SEUs. He suggested that the technique of environment stress screening might be effective. In this technique initial failures are artificially accelerated so that a plateau of stable operation is reached before an instrument is put in the field. Gabor Hadfi described his performance testing of the upgraded DCM 14 module that included some 470 tests at long-term, medium and low radiation exposures. For unshielded modules, the SEU rate was about 1.7 per hour; a 10cm-thick polyethylene-cadmium housing significantly lowered the rate. Field tests with shielding verified the laboratory results. In the final talk of the session, Steven Kadner discussed the reliability of mainstream operating systems, debunking the myth that reliability improves with time; rather, failures may increase due to lack of operating-system support for peripheral devices. He compared the performance of Microsoft systems with Linux, much preferring the latter for the IAEA’s work.

David Bot spoke about his experiences with Canadian safeguards instrumentation in the nuclear and space industries, with their very different requirements for failure rate and liability. Fitting the IAEA's needs into this spectrum, he advocated simple low-powered designs, deterministic operating systems for software, and multiple cross-linked processors and hardware watchdogs. Complex functionality could be layered on to the simple system. He highlighted the pitfalls in manufacturing and field support faced by the Agency, most due to lack of monies. James Halbig related LANLs experiences with developing fault-tolerant instrumentation for nuclear facilities in Kazakhstan. Starting with the stabilized assay meter (SAM), he describe several stages of instrument development at LANL that eventually produced the UNARM system, 72 of which are used at 10 sites worldwide and represent 564 instrument-operational years. As an optimal engineering practice, LANL employed fault-tolerant systems that function despite the failure of one or more components. Ed Hogan-Bassey drew parallels with the parameters of reliability needed for satellite-based communications systems and the associated SEU problems that should be considered if satellite communication is used to support IAEA remote monitoring systems.

Patrick Griffin explored options for hardening systems against radiation effects, urging that the IAEA consider them cost-justifiable at the design phase. For example, hardened silicon components are effective in certain applications. He presented evaluations showing critical charge production in the presence of various types of shielding, including polyethylene (with and without boron), lithium, and cadmium. Joe Wehlburg discussed radiation-tolerant processing techniques that are used in space systems. He recommended redundant systems with reusable or replaceable code using multiple processors, field programmable gate arrays (FPGAs), comparators, and storage and discussed testing, costs and design tradeoffs. As an example, he considered the implementation of an algorithm used in space-based systems that corrects images for distortion due to satellite rotation. Peter Chiaro described the large user facilities at ORNL, offering simulated radiation fields, environmental stress testing, and soon, a neutron source for exposing small devices. Jim Griggs discussed PNNL's physical facilities for testing radiation hardness, and the unique characterizations of nuclear-plant radiation and operating environments that had been done by PNNL. David Bailey discussed the environmental testing capabilities at Wyle Laboratory and reported on the testing of instrument systems and modules that had been done for the IAEA.

Seymour Morris was the first speaker to discuss processes that ensure reliability. He focussed on program management support, considering the Agency's option for ensuring their systems' lifetime reliability, from acquisition through operation, maintenance, and disposal. His company posted a reliability "toolkit" on their web site specifying essential and supplemental tests, and citing reference books and documents; these resources might be valuable to the IAEA. In a related presentation, Preston MacDiarmid specified similar methodology, including tools long used by the Department of Defense. He suggested that the problem of collecting data from remote sites might be addressed using MERIT, a comprehensive web-based system into which operators can directly enter data. David Nicholls explained the work of the DOD-funded Data Analysis Center for Software (DACS) in optimizing software applications. He believes that there is room for enormous improvements in software, and cited glaring examples of software unreliability that had caused failure in Patriot missile systems and problems with the baggage handling system that delayed the opening of the Denver airport. He discussed a number of the Center's tools that he thought could benefit the IAEA and cited the *DACS Software Reliability Sourcebook* that will be available on CD by the end of 2001.

The ensuing round-table discussion was an extension of the many spirited debates that had characterized the Workshop. The stage was set by Kelebnikov representing the IAEA's managerial viewpoint and concern with costs; he favored simple robust instruments for ensuring reliability. Speaking for the Agency's developers and engineers, Aparo welcomed the many possibilities offered by the new complex instrumentation despite its entailing greater resources and costs; more extensive training, record keeping and documentation of procedures; and its greater sensitive to environmental extremes. In the debate that followed, more suggestions were made for instruments, procedures, and management of tasks. Both speakers agreed that the meeting had demonstrated to the Agency that the best designs, expertise, and projects were available to them worldwide, through the Member State support programs. The Agency stated their intent to keep open the lines of communication, to better define their requirements, and adopt a more formal approach to procedures. They reiterated that the support of Member States, in addition to the IAEA’s regular budget, was essential for handling their continually growing workload. The session ended with a review of the IAEA’s observations and experience with SEU phenomena in safeguards instrumentation, and of the "lessons learned" in resolving many issues.

Jim Lemley and Mike Farnitano thanked the participants for their insightful and helpful contributions. They looked forward to future workshops.